REMARKS

The examiner states that: "**Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.**" Applicant therefore contends that the arguments in response to the prior action were persuasive.

The examiner also stated:

> **Examiner would like to point out that a preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478. 481 (CCPA 1951).**

Applicant does not understand the import of why the examiner has made this statement, but replies that the elements in the body of claims are used to distinguish the claims over the cited art, as set forth below.

Applicant also notes in passing that no amendment made herein was occasioned by the examiner's rejections over the prior art. Applicant has amended the claims to clarify subject matter therein. For example, the phrase an historical number of host pairs was missing from independent claims 1, 14, 24 and 28. In addition, the phrase "profile" in certain of those claims lacked antecedent basis. Thus, applicant made the amendments to the claims to address these minor omissions and the 112, second paragraph rejection. However, no amendment was made to overcome examiner's rejection rejections over the prior art. Accordingly, the next rejection cannot properly be a final rejection.[1]

35 U.S.C. §112

The examiner rejected Claims 1, 5, 12, 13, 14, 18, 28 and 32 rejected under 35 U.S.C. 112, second paragraph, as being indefinite. The examiner stated:

[1] See 706.07(a)Final Rejection, When Proper on Second Action [R-5]
*** Under present practice, second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims nor based on information submitted in an information disclosure statement filed during the period set forth in 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p). ***

> **The term "short and long" in claims 1, 5, 12, 13, 14, 18, 28 and 32 are relative terms which render the claims indefinite. The terms "long and short" are not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.**

Applicant disagrees. The terms long and short are properly used in the claims and defined by the specification. Nonetheless, in order to advance prosecution, Applicant has amended the claims to call for first and second update periods, as appropriate to overcome this rejection.

35 U.S.C. § 102

The examiner rejected Claims 1-36 under 35 U.S.C. 102(e) as being anticipated by Gupta et al. (US 7,234,168). The examiner stated:

> **As per claim 1, Gupta discloses: adding host-pair connection records to a connection table each time a host accesses another host (Column 10, Lines 26-44 and Liens 41-44); at the end of a short update period, accessing the connection table to determine new host pairs (Column 11, Lines 10-21); determining the number of new host pairs added to the table over the short update period (Column 11, Lines 10-21 and Column 11, Lines 23-37); and if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then indicating to a console that the new host is a scanner (Column 11, Lines 10-21).**

Applicant's claim 1 is directed to a method of detecting scanning attacks. Claim 1 includes the features of adding host-pair connection records to a connection table when a host accesses another host, at the end of a first update period, accessing the connection table to determine new host pairs; determining the number of new host pairs added to the table over the first update period; and if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs is smaller than the threshold number by a first factor value "C2", then indicating that the new host is a scanner.

The examiner argues that: "**... Gupta discloses: adding host-pair connection records to a connection table each time a host accesses another host (Column 10, Lines 26-44 and Liens 41-44);**." Applicant disagrees. At the cited passage Gupta discloses defining protocol vectors. These protocol vectors are comprise of the most often seen to the least often seen protocols.[2] Gupta neither at these passages nor elsewhere suggests, much less describes a connection table and in particular "adding host-pair connection records to a connection table when a host accesses another host."

The examiner argues that Gupta discloses: "**at the end of a short update period, accessing the connection table to determine new host pairs (Column 11, Lines 10-21).**" Applicant again disagrees. Gupta, at that passage, discloses keeping a run-time count of requests and packet separately and establishing a rate profile. Neither of these teachings suggests much less describes: "at the end of a first update period, accessing the connection table to determine new host pairs ... ."

The examiner argues that Gupta discloses: "**determining the number of new host pairs added to the table over the short update period (Column 11, Lines 10-21 and Column 11, Lines 23-37).**" Applicant again disagrees. At col. 11, lines 10-21, Gupta discloses keeping a run-time count of requests and packets and establishing a rate profile, as discussed above. At Col. 11, lines 23-37, Gupta discusses collection of statistical on protocol fields and signature processing. Neither of these teachings however suggest the feature of "determining the number of new host pairs added to the table over the first update period."

Finally, the examiner argues with respect to claim 1 that Gupta discloses: "**... if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then indicating to a console that the new host is a scanner (Column 11, Lines 10-21).**" Applicant disagrees. At that passage Gupta discloses:

> **By identifying the set of commonly used request-response packet pairs and creating a simple balance profile, the anomaly detector 62 detects most attacks. This is accomplished by: (1) keeping a run-time count of request and response packets separately, (2) establishing a rate profile for the occurrence of these individual packets and generate an alert if the threshold of deviation is crossed, and then (3) correlate the request and response by simply checking the balances. Request-response examples include: TCP SYN-TCP SYN & ACK; TCP FIN--TCP FIN & ACK; CIMP ECHO REQ--ICMP ECHO REPLY, ARP request--ARP response, DNS query query response, HTTP request--response.**

Neither in the passage above nor elsewhere in Gupta is there disclosed the threshold on host pairs or the value are used in accessing whether a new host is a scanner. Nothing in that

[2] Gupta col. 10, line 38.

passage deals with connection pairs, or a host making more than a first threshold number "C1" host pairs, that is smaller than the threshold number by a first factor value "C2."

Claim 8

In rejection of claim 8 the examiner stated:

> **As per claim 8, Gupta discloses: retrieving from a connection table logged values of protocols and ports used in host pair connections records in the table (Column 11, Lines 10-21); determining if the number of ports used in the historical profile is considerably smaller by a factor "C 1" than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold "C2", to record the anomaly (Column 11, Lines 10-21); and reporting a port scan to a console (Column 12, Lines 1-8).**

Claim 8 is directed to a method of detecting port scanning attacks and includes the features of retrieving from a connection table logged values of protocols and ports used in host pair connections records in the table, determining if the number of ports used in an historical profile is smaller by a factor "C1" than a current number of ports being scanned by a host, and if the current number is greater than a lower-bound threshold "C2"; recording that the current number for the host is greater than a lower-bound threshold as an anomaly; and reporting a port scan.

The examiner argues that Gupta discloses: **"retrieving from a connection table logged values of protocols and ports used in host pair connections records in the table (Column 11, Lines 10-21)** " Applicant disagrees. As argued above Gupta does not have any structure that is analogous to or the equivalent of a connection table. Moreover, at the cite passage Gupta does not disclose retrieving logged values of protocols and ports used in host pair connections, but instead discloses a run-time count of requests and packets and establishing a rate profile, as discussed above.

The examiner also argues that Gupta discloses: **determining if the number of ports used in the historical profile is considerably smaller by a factor "C1" than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold "C2", to record the anomaly (Column 11, Lines 10-21)."** Applicant contends that Gupta rather discloses run-time count of requests and packets and establishing a rate profile, as discussed above.

The examiner argues that Gupta discloses: **reporting a port scan to a console (Column 12, Lines 1-8)”** While, arguably Gupta mentions this feature, Gupta does not suggest any of the features of detecting a port scan as set forth in this claim. Instead, Gupta uses signature analysis of packets to look for illegal combination of code bits.[3] Applicant in contrast describes and claims a technique in which connection patterns between and among hosts in a network are analyzed, as set forth above.

Claim 14 is the computer program product analogue to claim 1 and is allowable for analogous reasons over Gupta.

Claim 20 is the computer program product analogue to claim 8 and is allowable for analogous reasons over Gupta, whereas claim 33 is the apparatus analogue to claim 8 and is also allowable over Gupta for analogous reasons as those given in claim 8.

Claim 24 is the computer program product analogue to claim 1 and claim 28 is the apparatus analogue to claim 1 and are allowable over Gupta for analogous reasons..

As for claim 2, 15, 25 and 29 Gupta does not disclose these thresholds "Cl" and "C2" and therefore cannot disclose that they are adjustable thresholds whether at Column 6, Lines 37-44 or elsewhere.

As for claims 3, 16, 26 and 30, Gupta does not disclose “the connection table” and therefore cannot disclose “a current time-slice connection table” or that “host pair records are added to the current time slice connection table whether at column 11, lines 14-15 or elsewhere. Note that the examiner alludes to rate profile as disclosing this feature. However, rate profile deals with packets not connections.

As for claims 4, 17, 27 and 31, Gupta does not disclose aggregating records from the current time-slice table into a second update period table whether at Column 10, Lines 35-45 or elsewhere. Gupta also does not check for ping scans at the end of a second update period or

[3] Another variable compares the protocol identification field to the finite set of known IP protocols; if the new protocol identifier is not recognized, this signals an anomaly. Yet another variable examines the set of TCP code bits to determine whether they contain legal bit combinations. Combinations other than legal ones signal an anomaly. For example, OS scanners are known to use strange combinations of code bits (e.g., SYN and FIN) to determine the target OS type.

indicate hosts which produced more than "C3" new host pairs over the second update period, as generally discussed above.

As for claim 5, 18; claims 6, 19; claims 11, 23 and 37: claim 12: and claim 13 each of these claims add distinct features because they deal with aspects of the connection table.

Claim 7 which deals with a ping type scan is not disclosed in Gupta, which seems only directed to a ping packet with multicasting destination.

Claims 9, 21 and 34 and Claims 10, 22 and 35, are allowable with their respective independent claims.

Accordingly, Applicant contends that the case in now in condition for allowance and such action is requested.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 12/15/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906